REMARKS

By this Amendment, claims 22-71 have been cancelled, without prejudice or disclaimer, and claims 72 to 108 have been added, all cancellations and/or additions merely to clarify the recited subject matter without any intention of narrowing the scope of any of the claims. Applicants have amended the currently pending claims in order to expedite prosecution and do not, by this amendment, intend to abandon subject matter of the claims as originally filed or later presented. Moreover, Applicants reserve the right to pursue such subject matter in a continuing application. Claims 1, 18-21 and 72-108 are pending in this patent application. Reconsideration of the rejections in view of the remarks below is requested.

In response to the constructive election of the present claims and the withdrawal of claims 22-71, Applicants have cancelled claims 22 to 71, without prejudice or disclaimer.

The Office Action rejected claims 1 and 21 under 35 U.S.C. §102(e) as being anticipated in view of U.S. Patent No. 5,745,574 ("Muftic"). Applicant respectfully traverses the rejection, without prejudice, and submits that Muftic fails to disclose, teach or suggest all the features recited by claims 1 and 21.

Muftic discloses a system that may have the ability to provide efficient key management and distribution in a secure manner by several different ways, more effective than existing models, and in a manner which protects public keys from tampering. (Muftic, col. 4, line 65 to col. 5, line 2). Muftic discloses that certification begins with a message sent from the station desiring certification to the certifying authority or by receiving that notification in any other way. Typically, this is done in a Certificate_Signature_Request message. The format of the Certificate_Signature_Request includes a certificate filled in with at least the public key which the requesting entity desires to have certified. The submission may be self-signed using the requestor's private key and transmitted to the CA for signature. When the CA receives the Certificate_Signature_Request, the information contained therein is validated in accordance with the policies established by a policy certification authority, and if the information is correct, the certifying authority issues a Certificate_Signature_Reply message returning to the requesting entity a signed certificate. When the requesting entity receives the Certificate_Signature_Reply message, it undertakes a Receive_Certificate process which verifies the signature on the certificate and stores it in a local certificate data base after verifying that the public key contained in the certificate corresponds to the entity's

private key. (Muftic, col. 11, lines 29-53). To verify the signature, the requesting entity has the public key of the certification authority. (Muftic, col. 12, lines 23-43).

The certification authority vouches for the identity of the public key owner, for the integrity of the public key itself, for the binding between the public key and the owner's identity, and optionally for some additional capabilities of the certificate owner in the electronic environment. This guarantee is reflected in the certificate through the identity of the authority, together with the authority's digital signature to the certificate. The signed certificates further may contain references to the types and purposes of public keys, to the relevant certification policies and eventually to the authorization privileges of certificate owners. (Muftic, col. 10, lines 45-55).

However, Muftic noticeably fails to disclose, teach or suggest, *inter alia,* denying access to a certification authority's public key and in response to a digital signing, permitting a recipient to utilize said public key as recited in claim 1.

In Muftic, the requesting entity has access to all public keys. Indeed, as noted above, the requesting entity sends a public key to the certification authority for certification and uses the public key of the certification authority to verify the certification. Thus, Muftic clearly fails to disclose, teach or suggest a requesting entity being denied access to a public key. Rather, in Muftic, with public keys widely available and accessible, the requesting entity merely seeks to confirm the identity of the owner of the public key and the integrity of the public key. The system in Muftic thus simply aims to prevent tampering (in the sense of modification) of a public key through the use of conventional signed certificates from one or more certifying authorities. In no way does the system in Muftic prevent access to or deny usage of a public key as public keys are widely available and accessible in the system of Muftic.

In contrast, the claimed invention of claim 1 denies access to a certification authority's public key and in response to a digital signing by the recipient, permits a recipient to utilize that public key. Thus, the claimed invention goes beyond preventing tampering and provides an additional or alternative protection mechanism.

Therefore, for at least the above reasons, Muftic fails to disclose, teach or suggest all the features recited by claim 1. Furthermore, claim 21 depends from claim 1 and is thus patentable at least for the same reasons as claim 1 and for the additional features recited therein. As a result, Applicant respectfully submits that the rejection under 35 U.S.C. §102(e) of claims 1 and 21 based on Muftic should be withdrawn and the claims allowed.

Further, the Office Action rejected claims 18 and 20 under 35 U.S.C. §103(a) as being obvious in view of Muftic and further in view of U.S. Patent No. 5,940,510 ("Curry et al."). Applicants respectfully traverse the rejection, without prejudice. Applicant respectfully submits that the teachings of Muftic and/or Curry et al. fail to disclose, teach or suggest all the features recited by claims 18 and 20.

Claims 18 and 20 depend from claim 1. Thus, these claims are patentable over Muftic alone for at least the same reasons as provided above in respect of claim 1 above and for the additional features recited therein.

Further, claims 18 and 20 are patentable over Curry et al. alone or in combination with Muftic because Curry et al., whether alone or in combination with Muftic, fail to disclose, teach or suggest, *inter alia,* denying access to a public key and in response to a digital signing, permitting a recipient to utilize said public key as recited in claim 1 from which both claims 18 and 20 depend.

Curry et al. disclose a secure device that may have the ability to store or create a private/public key set, whereby the private key never leaves the secure device and is not revealed under almost any circumstance. (Curry et al., col. 4, lines 49-52). However, Curry et al. clearly fail to disclose, teach or suggest denying access to a public key and further fail to disclose, teach or suggest, in response to a digital signing, permitting a recipient to utilize said public key. Since Muftic fails to disclose, teach or suggest the same, the disclosure and teachings of Curry et al. do not overcoming the shortcomings of Muftic, or vice versa.

Therefore, for at least the above reasons, Muftic and/or Curry et al. fail to disclose, teach or suggest all the features recited by claims 18 and 20. As a result, Applicants respectfully submit that the rejection of claims 18 and 20 under 35 U.S.C. §103(a) should be withdrawn and the claims allowed.

Applicants have added new claims 72 to 108. These new claims find support in the application, including, without limitation, at pages 44 to 50 of the specification. No new matter has been added. Further, claims 72 to 108 cover substantially related subject matter as claims 1 and 18-21 as they pertain to denying access to or utilization of a public key, activating a public key, or making a cryptographic capability available upon demonstration of agreement or consistency with one or more rules.

Claim 72 depends from claim 1 and is thus at least patentable by being dependent from claim 1 and for the additional features recited therein.

Claims 73 is patentable over the cited references at least because the cited references fail to disclose, teach or suggest a method of enforcing a security policy in a cryptographic

system, said policy requiring controlling use of a public key, said method comprising denying use of said public key, providing a recipient with a message containing rules of said cryptographic system, said rules including a rule regarding maintaining secrecy of said public key, and, in response to said recipient digitally signing said message, by which said recipient agrees to said rules, permitting said recipient to utilize said public key. Claims 74-78 depend from claim 73 and are thus patentable at least for the same reasons as claim 74 and for the additional features recited therein.

Claims 79 is patentable over the cited references at least because the cited references fail to disclose, teach or suggest a method of enforcing a security policy in a cryptographic system, said policy requiring controlling utilization of a public key, said method comprising providing a recipient with a message containing rules of said system and with a secure device containing an inactive form of said public key, wherein said public key cannot be obtained from said device, and in response to said recipient digitally signing said message, activating said public key in said secure device. Claims 80-84 depend from claim 79 and are thus patentable at least for the same reasons as claim 79 and for the additional features recited therein.

Claims 85 is patentable over the cited references at least because the cited references fail to disclose, teach or suggest, a method of enforcing a security policy in a cryptographic system, said policy including controlling use of a public key, said method comprising said recipient accessing a secure device, and in response to a predetermined transaction with said secure device, activating said public key in said secure device, said predetermined transaction including information from the secure device identifying operational capabilities of the secure device and uniquely identifying said secure device and further including information uniquely binding said recipient to said predetermined transaction, wherein said public key cannot be obtained from said secure device. Claims 86-94 depend from claim 85 and are thus patentable at least for the same reasons as claim 85 and for the additional features recited therein.

Claim 94 is patentable over the cited references at least because the cited references fail to disclose, teach or suggest, a rule system configured to control use by a participant in a cryptographic system of a cryptographic capability, the rule system including one or more rules from the following rules: a rule regarding maintaining secrecy of the cryptographic capability, a rule requiring payment upon each use of the cryptographic capability, a rule requiring payment upon each use of the participant's private key, a rule requiring payment

upon each certification of a certificate's status, a rule requiring payment for use of intellectual property provided through the cryptographic system, or a rule requiring payment upon each confirm-to transaction by the participant; wherein the rule system is configured to make the cryptographic capability available to the participant upon demonstration by the participant of agreement or consistency with the one or more rules. Claims 95-108 depend from claim 94 and are thus patentable at least for the same reasons as claim 94 and for the additional features recited therein.

All objections and rejections having been addressed, it is respectfully submitted that the present application is in condition for allowance. If questions relating to patentability remain, the Examiner is invited to contact the undersigned to discuss them.

Should any fees be due, please charge them to our deposit account no. 03-3975, under our order no. 061047/0264493. The Commissioner for Patents is also authorized to credit any over payments to the above-referenced deposit account.

Respectfully submitted,
PILLSBURY WINTHROP SHAW PITTMAN LLP

Jean-Paul G. Hoffman
Reg. No. 42,663
Tel. No. 703-905-2094
Fax No. 703-905-2500

JGH
P. O. Box 10500
McLean, VA 22102
(703) 905-2000